UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,460	08/04/2006	David Naccache	1032326-000404	5746

21839 7590 09/25/2009
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
09/25/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/588,460	NACCACHE, DAVID	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **8/11/09** has been entered.

Claims 1-15 have been canceled. Claims 16-30 have been added and are pending.

Response to Amendment

Claim Objections

Claim 27 is objected to because of the following informalities:

The term "at least one computer" should read as "the at least one computer" because this entity was already defined in parent claim 26.

Response to Arguments

Applicant's arguments with respect to claims 16-30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 16-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP Application Publication 2002/0069361 to Watanabe et al., hereinafter Watanabe in view of USP Application Publication 2001/0036301 to Yamaguchi et al., hereinafter Yamaguchi.

As per claim 16, Watanabe teaches a method of securing access to a piece of equipment, the method comprising:

creating a reference datum for an authorized user, in an authentication medium, wherein said reference datum comprises at least an encrypted authentic biometric signature [IDC] (0356);

acquiring, at a sensor, a plain biometric signature for a user requesting access to said piece of equipment (0357);

decrypting, in said authentication medium, said encrypted authentic biometric signature stored on said computer (0356);

verifying, in said authentication medium, the authenticity of said plain biometric signature by comparing said plain biometric signature of said user with said decrypted authentic biometric signature of an authorized user (0357); and

granting said user access to said piece of equipment if said comparison is successful and denying access if said comparison fails (0357). While Watanabe teaches many embodiments of securing access to a piece of equipment, he is silent in explicitly disclosing a single embodiment teaching all of the above mentioned limitations combined with storing said encrypted authentic biometric signature on a computer associated with said piece of equipment. Watanabe does teach storing the encrypted profile on computers in other embodiments. Moreover, Yamaguchi teaches that biometric templates are stored on a computer associated with said piece of equipment (see Figure 42 and paragraphs 0040 and 0044). Yamaguchi teaches hundreds of templates can be stored on a traditional computer database and hard drive. It is known that smart cards have limited memory. The claim would have been obvious because combining known methods which produce similar results is within the capabilities of one of ordinary skill in the art. Watanabe teaches the encrypted biometric signature is decrypted in the smart card; the same result is achieved whether it was always stored there, or was retrieved from a computer database.

As per claim 21, Watanabe teaches a method of securing access to a piece of equipment, the method comprising:

creating a reference datum for an authorized user in an authentication medium, wherein the creation of said reference datum (0198) comprises:

(i) inputting a personal identification code for said authorized user on a keyboard (0198 and 0248);

(ii) detecting, at a sensor, a plain authentic biometric signature for said authorized user (0198);

(iii) encrypting said plain authentic biometric signature by means of a private key (0198 and 0199);

(iv) sending said encrypted authentic biometric signature to a computer associated with said piece of equipment (0234);

(v) associating said personal identification code with said encrypted authentic biometric signature (0248); and

(vi) storing said encrypted authentic biometric signature and said associated personal identification code on said computer (0248);

receiving a personal identification code inputted on a keyboard (0248);

acquiring, at a sensor, a plain biometric signature of a user requesting access to said piece of equipment (0357); and

verifying the authenticity of said plain biometric signature for a user requesting access to said piece of equipment, wherein said verifying comprises:

(i) matching said personal identification code with an encrypted authentic biometric signature stored on said computer (0554);

(iii) decrypting said authentic biometric signature, on said authentication medium, by means of a secret key on said authentication medium (0357);

(iv) comparing, on said authentication medium, said decrypted authentic biometric signature with said plain biometric signature of said user requesting access to said piece of equipment, to provide a comparison result (0357); and

(v) granting access to said user requesting access to said piece of equipment if said comparison result is successful and denying access if said comparison result fails (0357).

While Watanabe teaching many embodiments of securing access to a piece of equipment, he is silent in explicitly disclosing a single embodiment teaching all of the above mentioned limitations combined with sending said encrypted authentic biometric signature, that is associated with said personal identification code, to said authentication medium. Watanabe does teach storing the encrypted profile on computers in other embodiments. Moreover, Yamaguchi teaches that biometric templates are stored on a computer associated with said piece of equipment (see Figure 42 and paragraphs 0040 and 0044). Yamaguchi teaches hundreds of templates can be stored on a traditional computer database and hard drive. It is known that smart cards have limited memory. The claim would have been obvious because combining known methods which produce similar results is within the capabilities of one of ordinary skill in the art. Watanabe teaches the encrypted biometric signature is decrypted in the smart card; the same

result is achieved whether it was always stored there, or was retrieved from a computer database.

As per claims 17 and 22, Watanabe teaches said authentication medium is an electronic card (0356).

As per claims 18 and 23, Watanabe teaches said electronic card includes a decryption module (0356).

As per claims 19 and 24, Watanabe teaches said electronic card includes a comparison module, and said comparing is performed in said electronic card (0357).

As per claims 20 and 25, Watanabe teaches said electronic card further comprises an encryption module (0346 and 0352).

As per claim 26, Watanabe teaches a device for securing access to a piece of equipment, comprising:

at least one computer, associated with said piece of equipment, for storing an encrypted authentic biometric signature (0234) and a corresponding personal identification code of an authorized user (0554);

a sensor for acquiring a plain biometric signature of a user requesting access to said piece of equipment (0357); and

an authentication medium having a controller, wherein said controller:

decrypts said authentic biometric signature by means of a secret key (0356);

compares said decrypted authentic biometric signature with said plain biometric signature of said user requesting access to said piece of equipment, to provide a comparison result; and grants access to said user requesting access to said piece of equipment if said comparison is successful and denying access if said comparison fails (0357).

While Watanabe teaching many embodiments of securing access to a piece of equipment, he is silent in explicitly disclosing a single embodiment teaching all of the above mentioned limitations combined with receiving said encrypted authentic biometric signature, associated with said personal identification code **in the authentication medium**. Watanabe does teach storing the encrypted profile on computers in other embodiments. Moreover, Yamaguchi teaches that biometric templates are stored on a computer associated with said piece of equipment (see Figure 42 and paragraphs 0040 and 0044). Yamaguchi teaches hundreds of templates can be stored on a traditional computer database and hard drive. It is known that smart cards have limited memory. The claim would have been obvious because combining known methods which produce similar results is within the capabilities of one of ordinary skill in the art. Watanabe teaches the encrypted biometric signature is decrypted in the smart card; the same result is achieved whether it was always stored there, or was retrieved from a computer database.

As per claim 27, Watanabe teaches at least one computer for storing a plurality of encrypted authentic biometric signatures and a corresponding plurality of personal identification codes for a corresponding plurality of authorized users [inherent this registration process applies to more than one user; 0234], wherein said at least one computer:

Watanabe does not explicitly teaches delivering an encrypted authentic biometric signature to said authentication medium when receiving an access request from a user, such that said authentication medium is capable of providing a plurality of users secure access to said piece of equipment. Examiner supplies the same rationale for combining the feature of storing the signatures in a computer until the access attempt as taught by Yamaguchi and recited in claim 26.

As per claim 28, Watanabe teaches said authentication medium is an electronic card having a memory storing a secret key that cannot be read from outside [smart cards are known for their protected memory].

As per claim 29, Watanabe teaches an encryption module that encrypts an authentic biometric signature supplied in plain form to said sensor and delivers said encrypted authentic biometric signature to said at least one computer, in response to an encryption command (0234).

As per claim 30, Watanabe teaches said secret key is a private key having a matching public key, and wherein said encryption module is included in said at least one computer and uses said matching public key (0235).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431